2014 Xilinx Security Working Group (XSWG) Agenda[1]

3100 Logic Drive, Summit Retreat, Building B, 2nd Floor, Longmont, CO 80503

Tuesday October 28, 2014		
Topic	**Presenter**	**Time Slot**
Check-in & Continental Breakfast		07:45 – 08:30
Welcome & Introductions	**Jason Moore** Director: Mkt Segment Engineering, Xilinx	08:30 – 09:00
Keynote Address *Ed Paradise, Vice President of Engineering for Cisco's Security and Trust Organization will lead the keynote forum on the topic of* ***Trustworthy Systems and FPGA Security****.* *The threat landscape is changing. Adversaries are becoming more aggressive and leveraging multiple attacks at the same time. Trustworthy Systems is the foundation for creating a secure environment. It requires all policies processes and technologies in the vendors environment to be security minded as well as the company's employees, partners, and suppliers understanding security is an implicit input into every question. With the increasing number of security data breaches around the world, security has grown to be a number one concern among our customers and a top investment priority for Cisco.*	**Ed Paradise** VP of Engineering, Cisco Systems	09:00 – 09:45
Security In Reconfigurable Systems *An overview from Horst Görtz Institute for IT-Security on countermeasures to harden devices against power side-channel attacks. Countermeasure techniques discussed include means for hiding and masking using implementations such as noise generation, clock dis-alignment, power equalization, and concurrent masking schemes. Evaluation of effectiveness will be provided, along with a summary including a brief discussion on physically secure systems on PSoCs.*	**Prof. Dr.-Ing. Tim Güneysu** **Dept EE/IE** Ruhr-University Bochum	09:45 – 10:15
Break		10:15 – 10:30
Vulnerabilities and Mitigations *This session will illustrate (at a high level), the most common FPGA/SoC security vulnerabilities and which mitigations are "in the box" from a Xilinx perspective. It will also discuss "out of the box" security vulnerability and mitigation concerns as well as research and development in those areas.*	**Jason Moore** Director: Mkt Segment Engineering, Xilinx	10:30 – 11:15
Supply Chain Threats and Issues *Xilinx dedicates significant resources to ensure that the fabrication and delivery of products are protected from tamper related mischief. The presentation discusses an overview of the supply chain process and the means by which device integrity is secured.*	**Alex Brown** VP: Supply Chain Xilinx	11:15 – 12:00
Lunch		12:00 – 13:00

Tuesday October 28, 2014		
Topic	**Presenter**	**Time Slot**
Ultrascale Silicon *This presentation presents the new security features that are available with the UltraScale FPGAs. New security features dealing with encrypted bitstream performance, public key authentication of bitstreams, Differential Power Analysis (DPA) protections, key agility, tamper logging and obfuscated key storage will be discussed.*	**Jim Wesselkamper** Sr. Staff Applications Engr. Xilinx	13:00 – 13:30
eFUSE Programming Infrastructure *An overview presentation of 7-Series, Zynq, and Ultrascale eFUSE features and implementations. Discussion of different e-FUSEs and their roles, programming and boot review, key management, tamper awareness and response.*	**Bryan Penner** Field Applications Engr. Xilinx	13:30 – 14:15
Break		14:15 – 14:30
Secmon and Secmon Proxy *Xilinx Security Monitor (SecMon) IP is an agency-evaluated and exportable security solution that meets the security needs of both defense-related and commercial products. The fully autonomous soft core continuously monitors for signs of post configuration tampering and can carry out penalties that render designs inaccessible. Now in is 6th generation of development, this discussion will highlight the major features of this security core and its corresponding SecMon Proxy (SMP) core.*	**Trevor Hardcastle** Staff Applications Engr. Xilinx	14:30 – 15:15
PUF Xilinx Study *This presentation covers the results of the Xilinx trade study on PUF technology. The study performs a comparative analysis of the current state of PUF technology and examines how applicable various PUF technologies are to Xilinx-specific use cases.*	**Jim Wesselkamper** Sr. Staff Applications Engineer, Xilinx	15:15-15:45
New Architectures for PUF Authentication and Key Generation *Silicon Physical Unclonable Functions (PUFs) have two main use cases: authentication and key generation. We discuss a new PUF authentication architecture, called noise-bifurcation, where a machine learning adversary sees an increasingly noisy challenge/response pair training set as security is scaled up, while the verifier sees constant noise. We then discuss a new PUF key generation architecture, using optimal symbol decoding, which has orders of magnitude better performance than existing schemes using techniques such as code-offset BCH and repetition coding.*	**Meng-Day (Mandel) Yu** Technical Director, Verayo, Inc.	15:45 – 16:15
XSWG2014 – Day 1 Wrap-up	**Jason Moore**	16:15 – 16:30
Evening Social: "Shupe Homestead, Colorado Ranch"		18:00 – 21:00

Directions from Xilinx Longmont to Shupe Homestead

From: 3100 Logic Dr, Longmont, CO 80503-7596 US
To: 11931 N 61st St, Longmont, CO 80503-9139 US

DRIVING DIRECTIONS

A) 3100 Logic Dr, Longmont, CO 80503-7596 US

---

1. Start out going north on S Fordham St toward Prospect Rd. (go 0.37 miles)
2. Take the 2nd left onto Pike Rd.
   - Pike Rd is 0.3 miles past Prospect Rd
   - If you reach Clover Basin Dr you've gone about 0.4 miles too far

(go 0.51 miles)

3. Take the 3rd right onto S Airport Rd.
   - S Airport Rd is just past Wildrose Dr
   - If you reach Arezzo Dr you've gone about 0.3 miles too far

(go 1.12 miles)

4. Turn left onto Nelson Rd.
   - Nelson Rd is 0.1 miles past Staghorn Dr
   - Allstate Insurance - Bob Silk is on the right
   - If you are on Airport Rd and reach Rogers Rd you've gone about 0.3 miles too far

(go 1.26 miles)

5. Turn right onto N 75th St.
   - N 75th St is 0.3 miles past Disc Dr
   - If you reach N 65th St you've gone about 1.2 miles too far

(go 2.44 miles)

6. Turn left onto Hygiene Rd.
   - Hygiene Rd is 0.2 miles past Gated Driveway
   - If you reach Rozena Dr you've gone about 0.6 miles too far

(go 1.74 miles)

7. Turn right onto N 61st St (Portions unpaved).
   - If you reach N 59th St you've gone about 0.2 miles too far

(go 0.17 miles)

8. 11931 N 61ST ST is on the left. (go 0 miles)

B) 11931 N 61st St, Longmont, CO 80503-9139 US

>> TOTAL ESTIMATED TIME: 13 minutes | DISTANCE: 7.61 miles

Wednesday October 29, 2014		
Topic	**Presenter**	**Time Slot**
Continental Breakfast		07:30 – 08:30
Day 2 Kickoff	**Jason Moore**	08:30 – 08:45
Zynq Secure Boot *This session will describe the Zynq Secure Boot process which provides Confidentiality, Integrity and Authentication of the configuration files. Implementation details will be covered and collateral identified. The session wraps up with a proposal on how public key authentication can be used to provide protection against side channel attacks.*	**Jason Moore**	08:45 – 09:30
Ronaldo MPSoC *This session will describe the security features of the Zynq UltraScale MPSoC device. This is the next generation SoC device after Zynq.*	**Jason Moore**	09:30 – 10:30
Break		10:30 – 10:45
Safe and Secure Hypervisor Technology (Sysgo) *A presentation of the development and use of a Safe and Secure Hypervisor technology. The presentation will discuss, hypervisors, TrustZone support and hardware implementation with specific focus on the Zynq product line as well as emerging architectures. The presentation will address the need for Safety and Security in industry segments from Avionics to Automotive. Including an introduction to PikeOS concept as a technology. SYSGO will also have a ZYNQ demonstration utilizing TrustZone to separate an Android and Linux Guest.*	**Stuart Fisher** Technical Marketing Director, Sysgo AG	10:45 – 11:15
Field Update *What you should know before beginning a design but we didn't tell you! This session introduces the attendee to some of the key associated considerations, including available design resources, development software, and choosing the right silicon family and device.*	**Barrie Timpe** Field Applications Engineering, Xilinx	11:15 – 12:00
Lunch		12:00 – 13:00
(Lecture) DPA Lecture / UltraScale Specific : Room tbd *DPA is a method an adversary can use to extract a secret (e.g. AES Key) from an electronic device. This presentation will provide a general overview of DPA and discuss attack vectors and countermeasures specific to UltraScale FPGAs.*	**Ed Peterson** Sr. Staff Applications Engineer,Xilinx	13:00 – 13:30
(Pre-Lab Lecture) Zynq Security : Silverthorne Room *DPA is a method an adversary can use to extract a secret (e.g. AES Key) from an electronic device. This presentation will provide a general overview of DPA and discuss attack vectors and countermeasures specific to UltraScale FPGAs.*	**Lester Sanders** Embedded Applications Engineer,Xilinx	13:30 – 14:00

Wednesday October 29, 2014		
Topic	**Presenter**	**Time Slot**
(Lecture) Runtime Security / TrustZone, Hypervisor, Microkernel : Room tbd *This session covers all topics related to providing run-time security. Topics include Operating System types (Monolithic vs. Microkernel), TrustZone, Hypervisors, and programming Zynq's AXI interfaces to enforce isolation and separation of resources.*	**Dave Beal** Sr. Product Marketing Manager, Xilinx	13:00 – 14:30
(Lecture) Zynq Runtime Security / Usage Control *Runtime security enforces that untrusted applications obey desired policies. The mechanisms used to enforce these policies include monitoring the operation of the system itself and the use of its resources, protecting the confidentiality of sensitive data both at rest and in motion, or controlling the data flow with user applications to prevent leakages and misuse of system resources. Isolating sensitive components and data within a trusted base, and only allowing external access through limited, narrow interfaces does not support well such runtime security mechanisms. In this talk we introduce a solution that relies on the run-time security mechanisms available on Zynq to enforce usage control policies. We motivate our approach with a representative use case, present the framework, and formulate our assumptions in terms of hardware support. Finally, we report on our design and implementation for the Linux kernel using the ARM TrustZone security extensions leveraged by the Zynq ZC702 as Trusted Execution Environment (TEE).*	**Javier Gonzalez** Computer Scientist, PhD Candidate, University of Copenhagen	14:45 – 15:45
(Lecture) Trusted Platform Module for Zynq *Trusted Platform Module (TPM) is an established secure cryptoprocessor solution for storing digital keys and certificates. While it is widely used in laptops and set-top boxes (e.g., dm-crypt, Bitlocker), it has not yet gained much popularity in SoC. Still, embedded manufacturers struggle to incorporate a cryptoprocessor solution to their designs. What does it take to have a TPM in the Zynq? Is it realistic to integrate it in an existing Zynq design? In this talk we explore the different alternatives to have a TPM on Zynq, look at the security impact of each one, and discuss how they can be implemented. In the process, we revisit some of the false assumptions made around TPM that can lead to security flaws.*	**Javier Gonzalez** Computer Scientist, PhD Candidate, University of Copenhagen	15:45 – 16:45
Closing Comments and Adjournment	**Jason Moore**	16:45 – 17:00

Wednesday October 29, 2014	
Lab Topic[2]	**Proctors**
Lab Notes : 1) The lab session will be a self-pace lab in Silverthorne. Please feel free to come and go to best suit your schedule. Lab sessions start immediately after Zynq Security presentation in Silverthorne. ~ 2) Xilinx processor specialists w/Zynq experience should expect each lab to take 30-45 minutes each. For those with FPGA experience only, each Zynq-7000 lab may take 60-90 minutes. 3) Laptops will be provided; please accommodate two users per laptop. 4) Registrants may opt to load a VMWare image onto their personal laptops if they wish to use their own PCs.	
Lab 1: UltraScale Bitstream Lab	**Lester Sanders** **Jim Wesselkamper**
Lab 2 : Changing Crypto Key in Zynq-7000	
Lab 3 : Secure System Update in Zynq-7000	
Lab 4 : Run Time Integrity Check of System Memory in Zynq-7000	
Lab 5 : Protecting Sensitive Information in Zynq-7000	

[1] Presenters, topics, and time slots subject to change – the final agenda will be supplied at the start of the XSWG.

[2] Labs run in parallel with the afternoon presentations on the 2nd day (labs located in the Silverthorne Conference room off the main Xilinx lobby). Seating is limited; please RSVP to Frank Wirtz frankw@xilinx.com to reserve your seat in the lab (on first-come first-serve basis).